FINDING PRIMITIVE ELEMENTS IN FINITE FIELDS OF SMALL CHARACTERISTIC

MING-DEH HUANG AND ANAND KUMAR NARAYANAN

ABSTRACT. We describe a deterministic algorithm for finding a generating element of the multiplicative group of the finite field $\mathbb{F}_{p^n}$ where p is a prime. In time polynomial in p and n, the algorithm either outputs an element that is provably a generator or declares that it has failed in finding one. The algorithm relies on a relation generation technique in Joux's heuristically $L(1/4)$-method for discrete logarithm computation. Based on a heuristic assumption, the algorithm does succeed in finding a generator. For the special case when the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ is small (that is $(\log_p(n))^{\mathcal{O}(1)}$), we present a modification with greater guarantee of success while making weaker heuristic assumptions.

1. INTRODUCTION

Let p be a prime and n a positive integer. The multiplicative group $\mathbb{F}_{p^n}^\times$ of the finite field $\mathbb{F}_{p^n}$ is cyclic and has $\varphi(p^n-1)$ generators (also called primitive elements), where φ is the Euler's totient function. Since $\varphi(p^n-1) = \Omega(\frac{p^n-1}{\log(\log(p^n-1))})$ [13], a large fraction of elements of $\mathbb{F}_{p^n}^\times$ are generators. In spite of their abundance, finding one efficiently remains an important open problem. The difficulty lies in testing if a given element is a generator and all known algorithms for testing either factor p^n-1 or solve an instance of the discrete logarithm problem in $\mathbb{F}_{p^n}^\times$, both of which are difficult.

Even if the question is relaxed and an element of large order is sought, approaches that work in general for every p and n are rare. Gao [9] presents an algorithm that produces an element of order $\exp(\Omega(\log n)^2/\log(\log(n)))$. Gao's algorithm is efficient conditioned on a conjecture which bears resemblance to our heuristic 2.1. Voloch [23] presents an approach suited to small p that finds an element of order $\exp(\Omega(\sqrt{n}))$. Notably, no previous algorithms to compute an element of order exponential in n were known, even if allowed to make heuristic assumptions.

There are other constructions that provably find an element of large order, but they only apply to very special (p,n) pairs [25][1][6][5][3][18][19]. For certain (p,n) pairs, von zur Gathen and Shparlinski [25] introduced the idea of constructing elements of high order using Gauss periods. Extensions and improvements on their results appear in [1][3][18][19]. When $n = \frac{p^c-1}{p-1}$ for some $c > 1$, Cheng, Gao and Wan [5] describe a deterministic algorithm that finds an element of order $\exp(\Omega(\sqrt{p^c}))$ in time polynomial in p^c. Voloch [24] and Chang [4] present constructions based on elements appearing as coordinates of points on certain curves.

Computer Science Department, University of Southern California, mdhuang@usc.edu .
Computer Science Department, University of Southern California, aknaraya@usc.edu .

An alternate relaxation of the question is to find small sets that contain a generator. Davenport [8] proved that when p is large enough compared to n and $\mathbb{F}_{p^n} = \mathbb{F}_p[\theta]$, the set $\mathbb{F}_p + \theta$ contains a generator of $\mathbb{F}_{p^n}^{\times}$. Shoup [20] extended this result to prove the existence of a subset $A \subseteq \mathbb{F}_{p^n}$ of size polynomial in p and n that contains a generator. Further, the set contains elements of degree bounded by $\mathcal{O}(\log_p(n))$ when represented as polynomials in θ. Shparlinski in [21] gave a simpler more efficient construction and in [22] further reduced the size of the subset A. The question remains on how to identify a generator given a small set that contains one.

In recent breakthroughs, Gologlu, Granger, McGuire, Zumbragel [10] and Joux [14] independently devised algorithms that assuming certain widely believed heuristics compute discrete logarithms in small characteristic finite fields faster than previously known. The authors of [10] demonstrated their algorithm by computing discrete logarithms in $\mathbb{F}_{2^{1971}}$ which at the time of announcement was a record [11]. Joux's algorithm is the first to compute discrete logarithms in heuristic $L(1/4, o(1))$ time, where $L(\ell, c)$ is defined as $\exp((c + o(1))(\log(p^n)^{\ell})(\log\log(p^n))^{1-\ell})$. All previous algorithms required $L(1/3, o(1))$ time and this speed up allowed Joux [15] to compute discrete logarithms in $\mathbb{F}_{2^{4080}}$. Gologlu, Granger, McGuire and Zumbragel [12] then extended the record to $\mathbb{F}_{2^{6120}}$.

A remarkable feature shared by the algorithms is that they both consider a small set as the factor base, one that is of size polynomial in the extension degree. Further, if the extensions they consider are obtained by adjoining a root ζ, then the factor base contains the elements that can be represented as linear polynomials in ζ. Assuming their relation generation algorithms succeed, discrete logarithms of the factor base elements can be determined up to a common constant multiple.

We propose to use the factor base and relation generation technique in Joux's paper [14] to efficiently find generators in $\mathbb{F}_{p^n}^{\times}$ of small characteristic. Whereas the algorithm for discrete logarithm computation assumes a given generator of the entire group, our interest is to find such a generator. Our observation however is that if the collected relations among the elements of the factor base are found to determine a cyclic group, then a generator of the cyclic group can also be constructed (see 2.4). Thus the factor base does not necessarily have to contain a generator. It suffices if the factor base generates the whole multiplicative group, and this is indeed the case as we observe that a result of F.R.K Chung [7] nicely applies to our situation where the finite field can be considered as an extension over a large enough base field. Thus our algorithm, in time polynomial in p and n, either certifiably finds a generator or indicates that it has failed in doing so. Moreover assuming a slightly weaker heuristic assumption than what is implicitly assumed in Joux's method, our algorithm finds a generator in time polynomial in p and n (see Theorem 2.4). In addition to the heuristic reasoning provided in this paper, the success of Joux's method in breaking the record of discrete logarithm computation can be taken as a strong evidence in support of the heuristic assumption.

For instances where p is of small order in $(\mathbb{Z}/n\mathbb{Z})^{\times}$, we present a modified algorithm that is simpler to state and relies on fewer heuristic assumptions.

In terms of organization, section 2.1 discusses the representation and preprocessing steps and leads to 2.2 where a search procedure for the special representation of finite fields required by the relation generation algorithm is described. Section 2.3 is on picking a small subset that generates multiplicative group followed by sections 2.4 and 2.5 that describes the relation generation procedure culminating in an algorithm algorithm for computing a generator. The final section deals with special case when p is of small order in $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

2. Finding Primitive Elements

2.1. **Representation of the Finite Fields.** As an initial step, $\mathbb{F}_{p^n}$ is considered as being embedded in $\mathbb{F}_{q^{2n}}$, where q is chosen such that $n \leq q$. In particular, we set $q := p^m$, where $m := \lceil \log_p(n) \rceil$.

The field $\mathbb{F}_{q^{2n}}$ is constructed as $\mathbb{F}_{q^2}[\zeta]$, where ζ is a root of an irreducible polynomial $g(x) \in \mathbb{F}_{q^2}[x]$ of degree n that is of a special form (see section 2.1).

The algorithm then proceeds by finding an element γ such that $\langle \gamma \rangle = \mathbb{F}_{q^2}[\zeta]$. As a consequence, $\delta := \gamma^{(q^{2n}-1)/(p^n-1)}$ has order $p^n - 1$ generates the multiplicative group of $\mathbb{F}_p[\delta] \cong \mathbb{F}_{p^n}$.

Informally, an explicit representation of $\mathbb{F}_{p^n}$ is as an $\mathbb{F}_p$ vector space with a basis that allows efficient multiplication. For instance, regarding $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[\mu]$ where μ is a root of a known irreducible degree n polynomial is an explicit representation. Due to Lenstra [16][Thm 1.2], an isomorphism between two explicit representations of a field of size p^n can be computed deterministically in time polynomial in n and $\log(p)$. Thus a generator for any explicit representation of $\mathbb{F}_{p^n}$ can be found as the image of δ under an isomorphism.

2.2. **Searching for an Irreducible polynomial of a Special Form.** We seek polynomials $h_o, h_1 \in \mathbb{F}_{q^2}[x]$ of low degree such that the factorization of $h_1(x)x^q - h_0(x)$ over $\mathbb{F}_{q^2}[x]$ has an irreducible factor of degree n. Let $g(x)$ denote one such irreducible factor of degree n. The field extension $\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}$ is constructed as $\mathbb{F}_{q^2}[\zeta]$ where ζ is a root of $g(x)$. The motivation behind choosing g in this manner is that the identity $h_1(\zeta)\zeta^q - h_0(\zeta) = 0$ would later allow us to replace ζ^q with an expression consisting of the low degree polynomials $h_0(\zeta)$ and $h_1(\zeta)$.

As an example, when $n = q-1$, setting $h_1(x) = 1$ and $h_0(x) = \lambda x$ where $\langle \lambda \rangle = \mathbb{F}_q^{\times}$, yields $h_1(x)x^q - h_0(x) = x(x^{q-1} - \lambda)$, where $(x^{q-1} - \lambda)$ is irreducible of degree $q-1$. Consequently, for the special case when $ord_n(p)$, the order of p modulo n is small (say $(\log_p n)^{\mathcal{O}(1)}$), in the initial step, we can set $m := ord_n(p)$, $q := p^m$ and embed $\mathbb{F}_{p^n}$ in to $\mathbb{F}_{q^{2(q-1)}}$ and skip the search for h_0 and h_1.

For $r \geq n$, let $N_q(r,n)$ denote the number of polynomials over $\mathbb{F}_{q^2}$ of degree $r \geq n$ that have an irreducible factor of degree n. As a first approximation, $N_q(r,n)$ is the product of the number of ways of choosing an irreducible polynomial of degree n and the number of ways of choosing a polynomial of degree $r-n$. Since roughly a fraction of $\frac{1}{n}$ of all polynomials of degree n are irreducible, the probability

$P_q(r,n) := \frac{N_q(r,n)}{q^{2r}}$ that a random polynomial of degree r has an irreducible factor of degree n is about $\frac{1}{n}$. The following precise bound on $P_q(r,n)$ is proven in [9]

$$\frac{I_n}{q^{2n}}\left(1-\frac{I_n-1}{2q^{2n}}\right) \leq P_q(r,n) \leq \frac{I_n}{q^{2n}}$$

where I_n denotes the number of irreducible polynomials over $\mathbb{F}_{q^2}$ of degree n. Further, $\frac{I_n}{q^{2n}}$ tends to $\frac{1}{n}$ as n tends to infinity.

If we were to assume that a random polynomial of the form $h_1(x)x^q - h_0(x)$, where h_0 and h_1 are of degree at most d has an irreducible factor of degree n with probability $P_q(q+d,n)$, then choosing $d = \Theta(\log_{q^2}(n)) = \Theta(1)$ is sufficient to ensure the existence of the h_0 and h_1 that we seek and leads to the following heuristic.

Heuristic Assumption 2.1. *There exists a positive integer d such that for all prime powers q and for all positive integers $n \leq q$, there exists $h_0, h_1 \in \mathbb{F}_{q^2}[x]$ of degree bounded by d such that the factorization of $h_1(x)x^q - h_0(x)$ over $\mathbb{F}_{q^2}[x]$ has an irreducible factor of degree n.*

Search for $h_0(x), h_1(x)$ and $g(x)$: *Enumerate candidates for $h_0, h_1 \in \mathbb{F}_{q^2}[x]$ with each of their degrees bounded by d. For each candidate pair (h_0, h_1), factor $h_1(x)x^q - h_0(x)$ and if it has an irreducible factor of degree n, output h_0, h_1 and the factor of degree n and stop. If no such candidates are found, declare failure.*

The search algorithm terminates after considering at most $q^{2d} = q^{\mathcal{O}(1)}$ candidate pairs. Factoring each candidate $h_1(x)x^q - h_0(x)$ takes time polynomial in the degree $q+d$ [2]. Thus a h_0, h_1 and g of the desired form can be computed in $q^{\mathcal{O}(1)}$ time and $\mathbb{F}_q^{2n}$ can be constructed as $\mathbb{F}_{q^2}[\zeta]$ where ζ is a root of $g(x)$.

2.3. **Small Generating Set.** We next choose a small subset $S \subseteq \mathbb{F}_{q^2}[\zeta]$ that generates $\mathbb{F}_{q^{2n}}^{\times}$. F.R.K Chung proved that for all prime powers s, for all positive integers r such that $(r-1)^2 < s$, for all μ such that $\mathbb{F}_{s^r} = \mathbb{F}_s[\mu]$, the set $\mathbb{F}_s + \mu$ generates $\mathbb{F}_{s^r}^{\times}$ [7, Thm. 8][26, Ques 1.1]. Since $n \leq q$, setting $S := \mathbb{F}_{q^2} + \zeta$ ensures that the subgroup generated by S, $\langle S \rangle = \mathbb{F}_{q^{2n}}^{\times}$.

2.4. **The Relation Lattice and Primitive Elements.** Given that $\langle S \rangle = \mathbb{F}_{q^{2n}}^{\times}$, the next step is to determine the relations satisfied by the elements in S so that we can determine $\mathbb{F}_{q^{2n}}$ as the free abelian group $\mathbb{Z}^{|S|}$ modulo the relations.

For a technical reason, S is first extended to the set $F := h_1(\zeta) \cup \{\lambda\} \cup S$, where $\langle \lambda \rangle = \mathbb{F}_{q^2}^{\times}$. An identity in $\mathbb{F}_{q^{2n}}$ of the form $\prod_{\beta \in F} \beta^{e_\beta} = 1$ for integers e_β defines a relation vector $(e_\beta, \beta \in F)$ indexed by elements in F. Let Γ denote the $|F|$-dimensional $\mathbb{Z}$-lattice of all relation vectors. The lattice Γ determines the subgroup generated by F as $\langle F \rangle \cong \mathbb{Z}^{|F|}/\Gamma$. Since $\langle F \rangle = \mathbb{F}_{q^{2n}}^{\times}$, $\mathbb{F}_{q^{2n}}^{\times} \cong \mathbb{Z}^{|F|}/\Gamma$.

The relation search step attempts to determine the lattice Γ by collecting a set of N relation vectors. Let R be the N by $|F|$ matrix consisting of the relation vectors are rows and Γ_R the $\mathbb{Z}$-lattice generated by the rows of R. The Smith normal form of R gives the decomposition of $\mathbb{Z}^{|F|}/\Gamma_R$ into its invariant factors

$$\mathbb{Z}^{|F|}/\Gamma_R = \langle e(1) \rangle \oplus \langle e(2) \rangle \oplus \ldots \oplus \langle e(r) \rangle \oplus E_{free} \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^{|F|-r}$$

where r is the $\mathbb{Z}$-rank of R, E_{free} is a free $\mathbb{Z}$-module of rank $|F|-r$ and for $1 \leq i \leq r$, $e(i) \in \mathbb{Z}^{|F|}$ denotes a relation vector and d_i the order of $e(i)$ in $\mathbb{Z}^{|F|}/\Gamma_R$ and for $1 \leq i < r$, $d_i \mid d_{i+1}$. Let π_r denote $\prod_{\beta \in F} \beta^{e(r)_\beta}$.

If $r = |F|$, then $\mathbb{Z}^{|F|}/\Gamma_R$ is finite and in addition if $\prod_{1 \leq i \leq r} d_i = q^{2n} - 1$, then we can deduce that $\Gamma_R = \Gamma$. Since $\mathbb{F}_{q^{2n}}^{\times} \cong \mathbb{Z}^{|F|}/\Gamma$ is cyclic, if $r = |F|$ and $\prod_{1 \leq i \leq r} d_i = q^{2n} - 1$, we can conclude that for $1 \leq i < r$, $d_i = 1$ and π_r generates $\mathbb{F}_{q^{2n}}^{\times}$.

In general, Γ_R might only be a sub lattice of Γ. From the natural surjection

$$\mathbb{Z}^{|F|}/\Gamma_R \twoheadrightarrow \mathbb{Z}^{|F|}/\Gamma \cong \mathbb{F}_{q^{2n}}^{\times}$$

it follows that if $\mathbb{Z}^{|F|}/\Gamma_R$ is cyclic, then the of image π_r which is a generator of $\mathbb{Z}^{|F|}/\Gamma_R$ under the surjection generates $\mathbb{Z}^{|F|}/\Gamma$.

The lemma implies that all we need to do is test if $\mathbb{Z}^{|F|}/\Gamma_R$ is a finite cyclic group and if so output π_r. It does not matter if the order of $\mathbb{Z}^{|F|}/\Gamma_R$ is a multiple of $q^{2n} - 1$. To check if $\mathbb{Z}^{|F|}$ is cyclic, it suffices to check if $r = |F|$ and for $1 \leq i < r$ if $d_i = 1$.

2.5. **Joux's Relation Generation Algorithm.** The relation generation phase begins with the following identity over $\mathbb{F}_{q^2}[x]$

$$\prod_{\alpha \in \mathbb{F}_q} x - \alpha = x^q - x.$$

For $(a, b, c, d) \in \mathbb{F}_{q^2}^4$ such that $ad - bc \neq 0$, the substitution $x \mapsto \frac{a\zeta + b}{c\zeta + d}$ yields

$$\prod_{\alpha \in \mathbb{F}_q} \frac{(a - \alpha c)\zeta + (b - \alpha d)}{(c\zeta + d)^q} = \frac{(c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q}{(c\zeta + d)^{q+1}}$$

$$\Rightarrow (c\zeta + d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q.$$

Linearity of raising to the q^{th} power implies

$$(c\zeta + d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a^q\zeta^q + b^q) - (a\zeta + b)(c^q\zeta^q + d^q).$$

By substituting $\zeta^q = \frac{h_0(\zeta)}{h_1(\zeta)}$, the right hand side becomes

$$\frac{(ca^q - ac^q)\zeta h_0(\zeta) + (da^q - bc^q)h_0(\zeta) + (cb^q - ad^q)\zeta h_1(\zeta) + (db^q - bd^q)h_1(\zeta)}{h_1(\zeta)}.$$

Consider the numerator of the above expression as a polynomial $n(x) \in \mathbb{F}_{q^2}[x]$ evaluated at ζ. The degree of $n(x)$ is bounded by $d + 1$. If $n(x)$ factors in to linear factors over $\mathbb{F}_{q^2}[x]$, then we get the following relation in $\langle F \rangle$

$$(c\zeta + d)h_1(\zeta) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = n(\zeta).$$

The above expression can be written as a product of an element in $\mathbb{F}_{q^2}^{\times}$ times $h_1(\zeta)$ times a fraction of products of monic linear polynomials in ζ over $\mathbb{F}_{q^2}$ being equal to

1. By expressing the element in $\mathbb{F}_{q^2}^\times$ as a power of λ, we indeed get a relation in $\langle F\rangle$.

The reason for choosing to work over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$ is that for every choice of $a,b,c,d \in \mathbb{F}_q$, the relation it yields becomes $\zeta^q - \zeta = \prod_{\alpha\in\mathbb{F}_q}(\zeta-\alpha)$. Thus, we have to work over an extension of $\mathbb{F}_q$ where the q^{th} power map would be non trivial and $\mathbb{F}_{q^2}$ is the smallest such extension.

For an $e \in \mathbb{F}_{q^2}^\times$, the substitutions $x \mapsto \frac{a\zeta+b}{c\zeta+d}$ and $x \mapsto \frac{ae\zeta+be}{ce\zeta+de}$ are identical and will lead to the same relation. Thus, the possible choices for $a,b,c,d \in \mathbb{F}_{q^2}$, that could lead to distinct relations can at best be identified with elements in $PGL(2,q^2)$.

Further, the relations corresponding to an element in $PGL(2,q^2)$ and its product with an element in $PGL(2,q)$ are off by the relation corresponding to the identity $\zeta^q - \zeta = \prod_{\alpha\in\mathbb{F}_q}(\zeta-\alpha)$.

Thus the number of possible choices for a,b,c,d can be identified with elements in the group $PGL(2,q^2)/PGL(2,q)$ which has cardinality $q(q^2+1) = \Theta(q^3)$.[1]

Relation Generation: *For every $(a,b,c,d) \in \mathbb{F}_{q^2}^4$ such that $ad-bc \neq 0$, compute the numerator $n(x)$ and if it factors in to linear factors over $\mathbb{F}_{q^2}[x]$, add the relation as a row to the relation matrix R.*

Heuristic Assumption 2.2. *The generated relation lattice Γ_R is large enough to ensure that $Z^{|F|}/\Gamma_R$ is a finite cyclic group.*

Note that for every $\beta \in F$, we could add the relation $\beta^{q^{2n}-1} = 1$ to ensure that $Z^{|F|}/\Gamma_R$ is finite.

The probability that a random polynomial of degree at most $d+1$ factors into linear factors is roughly $\frac{1}{(d+1)!}$ [17]. If the numerator polynomials $n(x)$ that appear in the relation generation phase behave as random polynomials with respect to their probability of splitting in to linear polynomials, then the expected number of trials required to get a relation is $(d+1)!$. Since d is a constant independent of q and n, the expected number of rows of R is a constant fraction of $\Theta(q^3)$.

Since the dimension of the lattice $|F|$ is at most q^2+2 and Γ_R is the lattice generated by $\Theta(q^3)$ points, it is overwhelmingly likely that $\Gamma_R = \Gamma$, which makes the weaker claim of heuristic 2.2 even more plausible.

The relation generation step can be performed in $q^{\mathcal{O}(1)}$ time since the number of choices for (a,b,c,d) is at most $q^{\mathcal{O}(1)}$ and factoring the numerator polynomial is $q^{\mathcal{O}(1)}$ as it is of constant degree. We have to express the constant $\mathbb{F}_{q^2}^\times$ factor in the relation as a power of λ, but that can be accomplished by solving the discrete logarithm in $\mathbb{F}_{q^2}^\times$ exhaustively in q^2 time. All that remains is to determine if $\mathbb{Z}^{|F|}/\Gamma_R$ is a finite cyclic group by computing the Smith normal form of R. The Smith normal form computation can be performed in $q^{\mathcal{O}(1)}$ time since R has at most $\Theta(q^3)$ rows, at most q^2+2 columns and each entry is an integer bounded by q^2.

[1] We would like to thank Antoine Joux for pointing out the need to mod out by $PGL(2,q)$.

Testing Phase: *Compute the Smith normal form of R and if $\mathbb{Z}^{|F|}/\Gamma_R$ is a finite cyclic group, output π_r. Else, declare failure.*

To summarize, our algorithm either certifiably finds a generator or indicates that it has failed in doing so. If the heuristics 2.1 and 2.2 are true, then the algorithm finds a generator in time polynomial in q which is a polynomial in p and n.

2.6. **Reducing the Problem of Finding Generators to a Conjecture.** Since the generated relation lattice Γ_R depends on the choice of the polynomials h_0, h_1 and g, heuristic 2.2 implicitly claims that for every choice of h_0, h_1 and g, the corresponding $Z^{|F|}/\Gamma_R$ is a finite cyclic group. This assumption can be weakened significantly by using the following modified testing phase.

Modified Testing Phase: *Compute the Smith normal form of R and if $\mathbb{Z}^{|F|}/\Gamma_R$ is a finite cyclic group, output π_r. Else, continue with the search for a new choice of h_0 and h_1.*

With the modified testing phase, our algorithm succeeds if there exists a h_0 and h_1 of constant degree that result in a Γ_R that defines a finite cyclic group and we have the following theorem.

Theorem 2.3. *If there exists a positive integer d such that for all prime powers q and for all positive integers $n \leq q$, there exists $h_0, h_1 \in \mathbb{F}_{q^2}[x]$ of degree bounded by d such that the factorization of $h_1(x)x^q - h_0(x)$ over $\mathbb{F}_{q^2}[x]$ has an irreducible factor $g(x)$ of degree n, and the relation lattice Γ_R corresponding to h_0, h_1, g defines a finite cyclic group $\mathbb{Z}^{|F|}/\Gamma_R$, then a generator for $\mathbb{F}_{p^n}$ can be found deterministically in time polynomial in p and n.*

2.7. **The special case when p is of small order in $(\mathbb{Z}/n\mathbb{Z})^\times$.** For the special case when $ord_n(p)$, the order of p modulo n is $(\log_p n)^{\mathcal{O}(1)}$, we present a modification to the algorithm that results in a procedure that has a greater guarantee of success while assuming less.

In the initial step, set $m := ord_n(p)$, $q := p^m$ and embed $\mathbb{F}_{p^n}$ in to $\mathbb{F}_{q^{2(q-1)}}$. Set $h_1(x) = 1$ and $h_0(x) = \eta x$ where $\langle \eta \rangle = \mathbb{F}_q^\times$. Such an η can be found in $\mathcal{O}(q)$ time by exhaustive searching. Since $h_1(x)x^q - h_0(x) = x(x^{q-1} - \eta)$, where $(x^{q-1} - \eta)$ is irreducible of degree $q-1$, set $g(x) = x^{q-1} - \eta$.

Since the degrees of h_1 and h_0 are at most 1, the numerator $n(x)$ that appears in the relation search is of degree at most 2.

If the numerators $n(x)$ behave as random polynomials of degree 2 in terms of factorization, then they factor with probability $\frac{1}{2}$. Thus, we expect to get at least $q(q^2+1)/2$ relations. In fact, we can prove that we get at least q^2+q relations.

Consider the upper triangular subgroup G_U of $PGL(2, q^2)/PGL(2, q)$, that is, the subgroup whose elements have a representative of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where $a \in \mathbb{F}_{q^2}^{\times}, b \in \mathbb{F}_{q^2}$. The cardinality of G_U is $((q^2-1)q^2)/((q-1)q) = q^2+q$.

For an element in G_U corresponding to an $a \in \mathbb{F}_{q^2}^{\times}$ and a $b \in \mathbb{F}_{q^2}$, the numerator polynomial $n(x)$ we obtain is the linear polynomial

$$(a^q\eta - a)x + (b^q - b).$$

Thus, we are guaranteed at least q^2+q relations.

Likewise, by considering the subgroup G_L of $PGL(2,q^2)/PGL(2,q)$ consisting of elements with a lower triangular representative, we get q^2+q-1 more relations.

Thus far we have made no heuristic assumptions for this special case. The only assumption we make is that $\mathbb{Z}^{|F|}/\Gamma_R$ is finite cyclic. The dimension of the relation lattice F is q^2+1 and we get at least $2q^2+2q-1$ distinct relations. If the relations that we obtain are modeled as being drawn independently at random from Γ, then with overwhelming probability $\Gamma_R = \Gamma$.

As a final remark, instead of restricting the factor base F to monic linear polynomials in δ, we could also include the evaluations of quadratic irreducible polynomials in $\mathbb{F}_{q^2}[x]$ at δ, but only those that appear as factors of the $n(x)$ during the relation search. Further, the first time a degree two element is encountered, it can be expressed in terms of a product of linear factors. If a quadratic factor reappears then it implies a new relation between products of linear factors.

3. Acknowledgements

We would like to thank Antoine Joux and Igor Shparlinski for their comments and suggestions on an earlier version of this paper.

References

[1] O. Ahmadi, I. Shparlinski, J. F. Voloch, "Multiplicative order of Gauss periods", Intern. J. Number Theory, 6 (4), 2010, pp.877-882.
[2] E. R. Berlekamp, "Factoring Polynomials Over Finite Fields", Bell System Technical Journal 46 (1967): 18531859.
[3] M.-C. Chang, "Order of Gauss periods in large characteristic", Taiwanese J. Math., 17 (2013), 621–628.
[4] M.-C. Chang, "Elements of large order in prime finite fields", Bull. Aust. Math. Soc., (to appear).
[5] Q. Cheng, S. Gao and D. Wan," Constructing high order elements through subspace polynomials", Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2012), Pages: 1457-1463
[6] Q. Cheng, "On the construction of finite field elements of large order, Finite Fields and Their Applications", Vol 11, Issue 3, Pages 358-366, 2005.
[7] F.R.K Chung, "Diameters and Eigenvalues", J. Amer. Math. Soc. 2 (1989), no. 2, 187196.
[8] H. Davenport, "On primitive roots in finite fields", Quart. J. Math. (Oxford) 8 (1937), 308-312.
[9] S. Gao, Elements of provable high orders in finite fields, Proc. Amer. Math. Soc., 127(6):16151623, 1999.
[10] F. Gologlu, R. Granger, G. McGuire and J. Zumbragel, "On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $F_{2^{1971}}$", Cryptology ePrint Archive: Report 2013/074.
[11] F. Gologlu, R. Granger, G. McGuire and J. Zumbragel," Discrete Logarithms in GF(2^{1971})", NMBRTHRY List, Feb 2013.

[12] F. Gologlu, R. Granger, G. McGuire and J. Zumbragel," Discrete Logarithms in GF(2^{6120})", NMBRTHRY List, Apr 2013.
[13] G. H. Hardy and E. M. Wright, "An introduction to the theory of numbers", 5th ed., Oxford Univ. Press, 1984.
[14] A. Joux, "A new index calculus algorithm with complexity L(1/4+o(1)) in very small characteristic", Cryptology ePrint Archive: Report 2013/095.
[15] A. Joux, " Discrete Logarithms in GF(2^{4080})", NMBRTHRY List, March 2013.
[16] H.W Lenstra, "Finding isomorphism between finite fields", Math. Comp., 56 (1991), pp. 329347.
[17] D. Panario, X. Gourdon, P. Flajolet, "An Analytic Approach to Smooth Polynomials over Finite Fields", ANTS 1998: 226-236
[18] R. Popovych, "Elements of high order in finite fields of the form $\mathbb{F}_q[x]/\Phi_r(x)$'", Finite Fields Appl., 18 (2012), 700–710.
[19] R. Popovych, 'Elements of high order in finite fields of the form $\mathbb{F}_q[x]/(x^m - a)$', Finite Fields Appl., 19 (2013), 86–92.
[20] V. Shoup, "Searching for primitive roots in finite fields", Mathematics of Computation 58:369-380, 1992
[21] I. E. Shparlinski, "On primitive elements in finite fields and on elliptic curves", Matem. Sbornik, 181 (1990), 1196–1206 (in Russian).
[22] I. E. Shparlinski, "Approximate constructions in finite fields", Proc. 3rd Conf. on Finite Fields and Appl., Glasgow, 1995, London Math. Soc., Lect. Note Series, 1996, v.233, 313–332.
[23] J. F. Voloch. "On the order of points on curves over finite fields", Integers, 7, 2004.
[24] J. F. Voloch,"Elements of high order on finite fields from elliptic curves", Bull. Aust. Math. Soc., 81 (2010), 425–429.
[25] J. von zur Gathen, I. Shparlinski, "Gauss periods in Finite Felds", Proc. 5th Conference of Finite Fields and their Applications, Augsburg, 1999, Springer-Verlag, Berlin, (2001), 162-177.
[26] D. Wan, "Generators and irreducible polynomials over finite fields", Math. Comp. 66 (219) (1997) 11951212.